# SYSTEM MANAGEMENT INTERRUPT GENERATION UPON COMPLETION OF CRYPTOGRAPHIC OPERATION

## ABSTRACT OF THE DISCLOSURE

An SMI (System Management Interrupt) generation capability is added to the cryptographic verification operation utilized to verify an update of a system management utility, such as the BIOS update utility. With the addition of an SMI upon completion of a signature verification command, the SMI handler issues a signature verification request to a trusted platform module (TPM) and returns control to the controlling application with a status code indicating it should begin polling the SMI handler for status. Upon completion of the verification operation, the TPM issues the SMI. The SMI handler then queries the TPM for status. The SMI handler then updates its internal status and permits access to the requested resource assuming the verification is successful. Upon the next poll from the application, the SMI handler returns the status to the calling application, which would either continue or abort with the update operation.

A:\Austin_1-168179-v2!-Patent Application.WPD
07241:207:7036-P175US